S523-25

100TH CONGRESS
2d Session

SENATE

REPORT
100-599

THE VIDEO PRIVACY PROTECTION ACT OF 1988

OCTOBER 21 (legislative day, OCTOBER 18), 1988.—Ordered to be printed

Mr. BIDEN, from the Committee on the Judiciary, submitted the following

REPORT

[To accompany S. 2361, as amended]

The Committee on the Judiciary, to which was referred the bill (S. 2361) to preserve personal privacy with respect to the rental, purchase, or delivery of video tapes or similar audio visual materials, having considered the same, reports favorably thereon with an amendment in the nature of a substitute and recommends that the bill, as amended, do pass.

CONTENTS

	Page
I. Purpose	1
II. Legislative History	2
A. Privacy Statutes	2
B. Supreme Court Decisions	4
C. Introduction of the Bill	5
III. Discussion	5
A. Video Section	5
B. Library Section	8
C. Legislation	8
IV. Vote of the Committee	9
V. Text of S. 2361	9
VI. Section-by-Section Analysis	11
VII. Cost Estimate	15
VIII. Regulatory Impact Statement	16
IX. Changes in Existing Law	16

I. PURPOSE

To preserve personal privacy with respect to the rental, purchase or delivery of video tapes or similar audio visual materials.

II. Legislative History

A. PRIVACY STATUTES

The Video Privacy Protection Act follows a long line of statutes passed by the Congress to extend privacy protection to records that contain information about individuals. In each instance, Congress has expanded and given meaning to the right of privacy.

In response to the public's growing awareness and concern about the confidentiality of personal information mainained by credit reporting bureaus, Congress passed the Fair Credit Reporting Act of 1970, 15 U.S.C. 1681 et seq. That Act prohibits credit and investigation reporting agencies that collect, store and sell information on consumers from disclosing records to anyone other than authorized customers. The Act requires credit agencies to make records available to the person who was the subject of the particular records, the "record subject," and to provide procedures for correcting inaccurate information.

Four years later, Congress passed the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. 1232(g) et seq., known as "the Buckley Amendment." That Act requires schools and colleges to allow students access to student records, provides challenge and correction procedures, and sharply limits the disclosure of educational records to third parties.

That same year, Congress passed the landmark Privacy Act, codified, at 5 U.S.C. 552a. The Privacy Act was the first comprehensive legislation to protect the confidentiality of personal information stored by federal agencies. The central concern of the Privacy Act was that information obtained for one purpose may not be used for a different purpose without the individual's consent. In addition, the Act provided that the government shall not maintain secret records; individuals must know what files are maintained on them and how they are used, and individuals must be able to correct and update their files.

Nevertheless, the Act allowed disclosure of records for "routine uses" compatible with the purposes for which the records were collected. This clause was later interpreted so broadly that it undercut the privacy protections embodied in the Act.

A 1977 amendment to the Privacy Act mandated the creation of the Privacy Protection Study Commission to make a "study of the data banks, automated data processing programs, and information systems of governmental, regional, and private organizations, in order to determine the standards and procedures in force for the protection of personal information." P.L. 95–38. Based on its findings, the Commission was to recommend additional legislation necessary to protect individuals' personal privacy interests.

The Commission concluded that an effective national information policy must embody three principles: it must minimize intrusiveness, maximize fairness and create legitimate, enforcable expectations of confidentiality. *Personal Privacy in an Information Society,* at 13–21 (1977). The Commission's report outlined the need to protect a wide variety of records including insurance, financial, telephone, employment, education, taxpayer and medical records. As a general rule, the Commission recommended that organizations

which maintained a confidential records system be placed under a legal duty not to disclose the record without the consent of the individual, except in certain limited circumstances, such as pursuant to a search warrant or subpoena. Even in such instances, the Commission stated that the individual must have have the right to challenge the court order before disclosure of the record. *Id.* at 362–63.

The Tax Reform Act of 1976, 26 U.S.C. 6103, protects the confidentiality of individual tax returns and limits third-party disclosures primarily to federal and state tax authorities.

The Right to Financial Privacy Act of 1978, 12 U.S.C. 3401 et seq., a congressional response to *U.S.* v. *Miller,* 425 U.S. 35 (1976), and a direct outgrowth of the Privacy Commission's report, created an assertable privacy interest in personal financial records. The Act provides individuals with the right to notice of a request and challenge before a bank or other financial institution may disclose records to governmental agencies.

Congress passed the Privacy Protection Act of 1980, 42 U.S.C. 2000(a), to prohibit law enforcement agents from searching press offices if no one in the office is suspected of committing a crime. In reversing *Zurcher* v. *Stanford Daily,* 436 U.S. 547 (1978), Congress reaffirmed a privacy right.

The Electronic Funds Transfer Act of 1980, 15 U.S.C. 1693, et seq., requires that any institution providing electronic funds transfers or other bank services must notify its customers about third party access to customer accounts. It does not, however, create specific privacy safeguards.

In 1982, Congress passed the Fair Debt Collection Act, P.L. 97–365, requiring federal agencies to provide individuals with due process protections before federal debt information may be released to a private credit bureau.

The Cable Communications Policy Act of 1984, P.L. 98–549, prohibits a cable service from disclosing information about a subscriber's cable viewing habits without the individual's consent. The Act requires the cable service to inform the subscriber of the nature and use of personally indentifiable information collected; the disclosures that may be made of such information; and the period during which such information will be maintained. The cable service must also provide subscribers access to information maintained about them.

Senators Leahy and Mathias, and Congressmen Kastenmeier and Moorhead, introduced the Electronic Communications Privacy Act in 1985. It was enacted in 1986. The Electronic Communications Privacy Act, 18 U.S.C. 2510 et seq., amends the federal wiretap statute to prohibit the unauthorized interception and disclosure of electronic communications made possible by new technologies, such as cellular phones, electronic mail and satellite television transmissions. The law defines electronic communications, restricts disclosure of stored communications, and creates civil and criminal penalties for individuals who, without authorization, willfully intercept or disclose the contents of electronic communications or who access such communications while in electronic storage.

The Electronic Communications Privacy Act, generally regarded as the most advanced privacy legislation passed by the Congress

thus far, responsed to important issues concerning the use of new information, communication and computer technologies. It was supported by leading telecommunications and computer companies in the country, the American Civil Liberties Union, the Department of Justice, and over 20 national organizations, including the National Association of Manufacturers, the Chamber of Commerce and the Direct Marketing Association.

This session, Congress passed legislation to bring under the wing of the 1974 Privacy Act the computerized matching of personal information held in federal agency databases. For years, the computerized matching of records has grown outside the scope of government regulation and oversight. The Computer Matching and Privacy Protection Act of 1988, P.L. 100–503, will help close the loop hole created by the misinterpretation and misapplication of the 1974 Privacy Act's "routine use" exception.

B. SUPREME COURT DECISIONS

Justice Brandeis, in his famous dissent in *Olmstead* v. *United States,* 277 U.S. 438 (1928), warned of the danger that new technologies would chip away at traditional privacy safeguards:

> Subtler and more far-reaching means of invading privacy have become available to the Government. * * * The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.

Id. at 473–74.

In *Katz* v. *United States,* 389 U.S. 347 (1967), the Supreme Court adopted Justice Brandeis' concern about intrusion through wiretap, but did not address the various other technologies that might give rise to similar privacy concerns.

Acknowledging the relationship between the right of privacy and intellectual freedom is a central part of the first amendment. The Supreme Court recognized the important tie between the disclosure of lists that reveal personal and political beliefs and the first amendment right of association in *NAACP* v. *Alabama,* 357 U.S. 449 (1958). In that case, the Court held that Alabama could not obtain the membership lists of the NAACP, reasoning that "privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs." *Id.* at 462.

Protecting an individual's choice of books and films is a second pillar of intellectual freedom under the first amendment. In *Stanley* v. *Georgia,* 394 U.S. 557, 565 (1969), the Court declared, "If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his house, what books he may read or what films he may watch."

The Court stopped short of adopting an explicit right to personal information privacy. In *Whalen* v. *Roe,* 429 U.S. 589, 605 (1977), the Court recognized "the threat to privacy implicit in the accumula-

tion of vast amounts of personal information in computerized data banks or other massive government files" and the fact that officials charged with collection of such data have a duty, arguably rooted in the Constitution, to protect the subjects of the data from unwarranted disclosure. See also *Paul* v. *Davis,* 424 U.S. 693 712–13 (1976) (publicizing the fact of an arrest did not infringe arrestee's right to privacy).

C. INTRODUCTION OF THE BILL

Senators Leahy, Grassley, Simon, and Simpson introduced S. 2361 on May 10, 1988. Representative McCandless had introduced H.R. 3523 on October 21, 1987. On June 29, 1988, Congressman Kastenmeier introduced H.R. 4947. The Senate Judiciary Subcommittee on Technology and the Law and the House Judiciary Subcommittee on Courts, Civil Liberties, and the Administration of Justice held a joint hearing on S. 2361 and H.R. 4947 on August 4, 1988.

III. Discussion

The Video Privacy Protection Act of 1988 prohibits video service providers from disclosing personally identifiable information except in certain, limited circumstances. As a general rule, personally identifiable information may only be disclosed with the prior written consent of the individual.

A. VIDEO SECTION

The impetus for this legislation occurred when a weekly newspaper in Washington published a profile of Judge Robert H. Bork based on the titles of 146 films his family had rented from a video store. "The Bork Tapes," *City Paper,* Sept. 25–Oct. 1, 1987, at 1. At the time, the Senate Judiciary Committee was holding hearings on Judge Bork's nomination to the Supreme Court.

Members of the Judicary Committee denounced the disclosure. When Senator Simpson brought the matter to the Committee's attention, he said:

> I listen to us speak about the right of privacy with regard to *Roe* v. *Wade, Griswold* v. *Connecticut,* those kinds of cases, theory, dissents, majorities. And then I come across a fascinating article. Maybe this does not mean anything to anyone. * * * But let me tell you: It seems more real than anything I know about the right to privacy after practicing law for 18 years.

Hearings on Nomination of Robert H. Bork to be Associate Justice of the Supreme Court of the United States Before the Senate Committee on the Judiciary, 100th Cong., 1st Sess. 1372 (Sept. 28, 1987).

Senator Leahy joined with Senator Simpson in denouncing the disclosure:

> It is noboby's business what Oliver North or Robert Bork or Griffin Bell or Pat Leahy watch on television or read or think about when they are home. * * * [I]n an era of interactive television cables, the growth of computer checking and check-out counters, of security systems and

> telephones, all lodged together in computers, it would be relatively easy at some point to give a profile of a person and tell what they buy in a store, what kind of food they like, what sort of television programs they watch, who are some of the people they telephone. * * * I think that is wrong. I think that really is Big Brother, and I think it is something that we have to guard against.
>
> * * * * *
>
> [Privacy] is not a conservative or a liberal or moderate issue. It is an issue that goes to the deepest yearnings of all Americans that we are free and we cherish our freedom and we want our freedom. We want to be left alone.

Id. at 1374. *See also id.* at 1676–77 (letter from the ACLU); *Olmstead* v. *United States,* 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) (describing the right to be let alone as "the most comprehensive of rights and the right most valued by civilized man.").

Similar, though less well publicized, incidents have occurred. Jack Messer, vice-president of the Video Software Dealer's Association, stated that the attorney for a women in a child custody proceeding made an informal request for the records of every film rented by her husband in an effort to show that, based on his viewing habits, he was an unfit father. *The Philadelphia Inquirer,* Oct. 21, 1987, at 1.

S. 2361 helps define the right of privacy by prohibiting unauthorizd disclosure of personal information held by video tape providers. The bill attempts to give meaning to, and thus enhance, the concept of privacy for individuals in their daily lives.

As Senator Grassley said when S. 2361 was introduced:

> Privacy is something we all value. The right of privacy is not, however, a generalized undefined right: It is a specific right, one which individuals should understand. And it is the role of the legislature to define, expand, and give meaning to the concept of privacy. This bill will give specific meaning to the right of privacy, as it affects individuals in their daily lives.

134 Cong. Rec. S5400–01 (May 10, 1988).

Senator Simon pointed out:

> There is no denying that the computer age has revolutionized our world. Over the past 20 years we have seen remarkable changes in the way each one of us goes about our lives. Our children learn through computers. We bank by machine. We watch movies in our living rooms. These technological innovations are exciting and as a nation we should be proud of the accomplishments we have made.
>
> Yet, as we continue to move ahead, we must protect time honored values that are so central to this society, particularly our right to privacy. The advent of the computer means not only that we can be more efficient than ever before, but that we have the ability to be more intrusive than ever before. Every day Americans are forced to provide to businesses and others personal information without

> having any control over where that information goes. * * * These records are a window into our loves, likes, and dislikes.

Id. at S5401.

Senator Patrick Leahy also noted that the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of surveillance. *Id.* at S5399. *See also* D. Burnham, *The Rise of the Computer State* (1982). These "information pools" create privacy interests that directly affect the ability of people to express their opinions, to join in association with others, and to enjoy the freedom and independence that the Constitution was established to safeguard.

The bill prohibits video stores from disclosing "personnally identifiable information"—information that links the customer or patron to particular materials or services. In the event of an unauthorized disclosure, an individual may bring a civil action for damages.

The bill permits the disclosure of personally identifiable information under appropriate and clearly defined circumstances. For example, information may be disclosed in response to a court order, and companies may sell mailing lists that do not disclose the actual selections of their customers. The bill also preserves the rights of customers and patrons under state and local law.

In a joint hearing of the Senate Judiciary Subcommittee on Technology and the Law and the House Judiciary Subcommittee on Courts, Civil Liberties, and the Administration of Justice, held on August 3, 1988, Representatives Al McCandless, the sponsor of the first Video Privacy bill introduced, stated:

> There's a gut feeling that people ought to be able to read books and watch films without the whole world knowing. Books and films are the intellectual vitamins that fuel the growth of individual thought. The whole process of intellectual growth is one of privacy—of quiet, and reflection. This intimate process should be protected from the disruptive intrusion of a roving eye.

[Hearing Transcript at 10].

Janlori Goldman, counsel for the American Civil Liberties Union, testified:

> These precious rights have grown increasingly vulnerable with the growth of advanced information technology. The new technologies not only foster more intrusive data collection, but make possible increased demands for personal, sensitive information. Private commercial interests want personal information to better advertise their products. The government is interested in sensitive information to enhance political surveillance. And, the intelligence community may be looking at reading lists to protect our national security. The danger here is that a watched society is a conformist society, in which individuals are chilled in their pursuit of ideas and their willingness to experiment with ideas outside of the mainstream. Although

> Judge Bork recently joked about how embarrassed he is to have the world learn that he watches dull movies, imagine if his confirmation had been doomed by the revelation of more unsettling viewing habits.
>
> New technologies enable people to receive and exchange ideas differently than they did at the time the Bill of Rights was drafted. Personal papers once stored in our homes are now held by others with whom we do business. Transactional information may be easily stored and accessed. Records of our reading and viewing histories are now maintained by libraries, and cable television and video companies. The computer makes possible the instant assembly of this information.

[Written Testimony at 10–11].

B. LIBRARY SECTION

Although the original impetus for the legislation was the disclosure of Judge Bork's video rental list, the bill's sponsors, Senators Leahy, Grassley, Simpson and Simon, included a similar protection for library borrower records, recognizing that there is a close tie between what one views and what one reads.

The subcommittee reported a restriction on the disclosure of library borrower records similar to the one on video records. However, the committee was unable to resolve questions regarding the application of such a provision for law enforcement.

C. LEGISLATION

The Video Privacy Protection Act prohibits video tape service providers from disclosing personally identifiable information except in narrow and clearly defined circumstances. The Act allows consumers to maintain control over personal information divulged and generated in exchange for receiving services from video tape service providers. The Act reflects the central principle of the Privacy Act of 1974: that information collected for one purpose may not be used for a different purpose without the individual's consent.

The exceptions to the prohibition on disclosure in S. 2361 are narrowly tailored and clearly defined. They allow for disclosure of limited information with the individual's consent, for legitimate business purposes with the consumer's ability to prohibit such disclosure or pursuant to a court order.

The civil remedies section puts teeth into the legislation, ensuring that the law will be enforced by individuals who suffer as the result of unauthorized disclosures. It provides that an individual harmed by a violation of the Act may seek compensation in the form of actual and punitive damages, equitable and declaratory relief and attorneys' fees and costs.

Statutory damages are necessary to remedy the intangible harm caused by privacy intrusions. Simialr remedies exist in the federal wiretap statute as revised by this committee in 1986. The absence of such a remedy in the Privacy Act of 1974 is often cited as a significant weakness.

IV. VOTE OF THE COMMITTEE

On August 10, 1988, S. 2361 was approved for full committee consideration by the Subcommittee on Technology and the Law. On October 5, 1988, with a quorum present and by voice vote, the committee approved an amendment in the nature of a substitute and an amendment to the title cosponsored by Senators Leahy, Grassley, Simon, and Simpson. The Committee then unanimously ordered the bill (as amended) favorably reported.

V. TEXT OF S. 2361

A BILL To amend title 18, United States Code, to preserve personal privacy with respect to the rental, purchase, or delivery of video tapes or similar audio visual materials and the use of library materials or services

SECTION 1 SHORT TITLE.

This Act may be cited as the "Video Privacy Protection Act of 1988".

SEC. 2. CHAPTER 121 AMENDMENT.

(a) IN GENERAL.—Chapter 121 of title 18, United States Code, is amended—

(1) by redesignating section 2710 as section 2711; and

(2) by inserting after section 2709 the following:

"§ 2710. Wrongful disclosure of video tape rental or sale records

"(a) DEFINITIONS.—For purposes of this section—

"(1) the term 'consumer' means any renter, purchaser, or subscriber of goods or services from a video tape service provider;

"(2) the term 'ordinary course of business' means only debt collection activities, order fulfillment, request processing, and the transfer of ownership;

"(3) the term 'personally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider or library; and

"(4) the term 'video tape service provider' means any person, engaged in the business of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials, or any person or other entity to whom a disclosure is made under paragraph (b)(2)(D), but only with respect to the information contained in the disclosure.

"(b) VIDEO TAPE RENTAL AND SALE RECORDS.—(1) A video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for the relief provided in subsection (d).

"(2) A video tape service provider may disclose personally identifiable information concerning any consumer—

"(A) to the consumer;

"(B) to any person with the informed, written consent of the consumer given at the time the disclosure is sought;

"(C) to a law enforcement agency pursuant to a warrant issued under the Federal Rules of Criminal Procedure, an

equivalent State warrant, a grand jury subpoena, or a court order;

"(D) to any person if the disclosure is solely of the names and addresses of consumers and if—

"(i) the video tape service provider has provided the consumer with the opportunity, in a clear and conspicuous manner, to prohibit such disclosure; and

"(ii) the disclosure does not identify the title, description, or subject matter of any video tapes or other visual material; however, the subject matter of such materials may be disclosed if the disclosure is for the exclusive use of marketing goods and services directly to the consumer;

"(E) to any person if the disclosure is incident to the ordinary course of business of the video tape service provider; or

"(F) pursuant to a court order, in a civil proceeding upon a showing of compelling need for the information that cannot be accommodated by any other means, if—

"(i) the consumer is given reasonable notice, by the person seeking the disclosure, of the court proceeding relevant to the issuance of the court order; and

"(ii) the consumer is afforded the opportunity to appear and contest the claim of the person seeking the disclosure.

If an order is granted pursuant to subparagraph (C) or (F), the court shall impose appropriate safeguards against unauthorized disclosure.

"(3) Court orders authorizing disclosure under subparagraph (C) shall issue only with prior notice to the consumer and only if the law enforcement agency shows that there is probable cause to believe that the records or other information sought are relevant to a legitimate law enforcement inquiry. In the case of a State government authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the video tape service provider, may quash or modify such order if the information or records requested are unreasonably voluminous in nature or if compliance with such order otherwise would cause an unreasonable burden on such provider.

"(c) CIVIL ACTION.—(1) Any person aggrieved by any act of a person in violation of this section may bring a civil action in a United States district court.

"(2) The court may award—

"(A) actual damages but not less than liquidated damages in an amount of $2,500;

"(B) punitive damages;

"(C) reasonable attorneys' fees and other litigation costs reasonably incurred; and

"(D) such other preliminary and equitable relief as the court determines to be appropriate.

"(3) No action may be brought under this subsection unless such action is begun within 2 years from the date of the act complained of or the date of discovery.

"(4) No liability shall result from lawful disclosure permitted by this section.

"(d) PERSONALLY IDENTIFIABLE INFORMATION.—Personally identifiable information obtained in any manner other than as provided in this section shall not be received in evidence in any trial, hearing, arbitration, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision of a State.

"(e) DESTRUCTION OF OLD RECORDS.—A person subject to this section shall destroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information under subsections (b)(2) or (c)(2) or pursuant to a court order.

"(f) SELECTION OF A FORUM.—Nothing in this section shall limit rights of consumers or patrons otherwise provided under State or local law. A Federal court shall, in accordance with section 1738 of title 28, United States Code, give preclusive effect to the decision of any State or local court or agency in an action brought by a consumer or patron under a State or local law similar to this section. A decision of a Federal court under this section shall preclude any action under a State or local law similar to this section.".

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 121 of title 18, United States Code, is amended—

(1) in the item relating to section 2710, by striking out "2710" and inserting "2711" in lieu thereof; and

(2) by inserting after the item relating to section 2709 the following new item:

"2710. Wrongful disclosure of video tape rental or sale records.".

Amend the title to read as follows:

A bill to amend title 18, United States Code, to preserve personal privacy with respect to the rental, purchase, or delivery of video tapes or similar audio visual materials.

VI. SECTION-BY-SECTION ANALYSIS

SECTION 1

This bill, when enacted, may be cited as the "Video Privacy Protection Act of 1988."

SECTION 2

This section amends chapter 121 of title 18 of the United States Code by redesignating section 2710 as section 2711 and inserting after section 2709 a new section 2710.

Section 2710(a) sets out the definitions for the terms used in the Act. The term "consumer" means any renter, purchaser, or subscriber of goods or services from a video tape service provider. The term "ordinary course of business" means only debt collection activities, order fulfillment, request processing, and the transfer of ownership.

The term "personally identifiable information" includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider.

Unlike the other definitions in this subsection, paragraph (a)(3) uses the word "includes" to establish a minimum, but not exclusive, definition of personally identifiable information. The definition of personally identifiable information includes the term "video" to make clear that simply because a business is engaged in the sale or rental of video materials or services does not mean that all of its products or services are within the scope of the bill. For example, a department store that sells video tapes would be required to extend privacy protection to only those transactions involving the purchase of video tapes and not other products.

This definition makes clear that personally identifiable information is intended to be transaction-oriented. It is information that identifies a particular person as having engaged in a specific transaction with a video tape service provider. The bill does not restrict the disclosure of information other than personally identifiable information. Thus, for example, a video tape service provider is not prohibited from responding to a law enforcement agent's inquiry as to whether a person patronized a video tape service provider at a particular time or on a particular date.

The term "video tape service provider" means any person engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials, such as laser disks, open-reel movies, or CDI technology, or any person or other entity to whom a disclosure is made under subparagraphs (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure.

Section 2710(b)(1) establishes a statutory presumption that the disclosure of personally identifiable information is a violation of this section unless a permissible exception, as defined in Section 2710(b)(2), applies.

Section 2710(b)(2) sets out the six circumstances under which a video tape service provider may disclose personally identifiable information.

Under paragraph (2)(A), personally identifiable information may be disclosed directly to the consumer who is the subject of the information. This provision is in accord with a primary tenet of the 1974 Privacy Act that the subject of the record should be able to inspect such information held by third parties.

Under paragraph (2)(B), personally identifiable information may be disclosed to any person with the informed written consent of the consumer given at the time the disclosure is sought.

Under paragraph (2)(C), personally identifiable information may be disclosed to a law enforcement agency pursuant to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent state warrant, a grand jury subpoena, or a court order. Paragraph (3) makes clear that court orders authorizing disclosure under paragraph (2)(C) shall issue only with prior notice to the consumer and only if the law enforcement agency shows that there is probable cause to believe that the records or other information sought are relevant to a legitimate law enforcement inquiry. In the case of a State government authority, such a court order shall not issue if prohibited by the law of the State. A court issuing an order pursuant to this section, on a motion made promptly by the video

tape service provider, may quash or modify such order if the information or records requested are unreasonably voluminous in nature or if compliance with such order otherwise would cause an unreasonable burden on such provider.

If personally identifiable information is disclosed, pursuant to paragraph (2)(C), the court shall impose appropriate safeguards against unauthorized disclosure. For example, the court may require parties to the proceeding to agree not to disclose the information.

Under paragraph (2)(D), personally identifiable information may be disclosed to any person if the disclosure is solely of the names and addresses of consumers and if the video tape service provider has provided the consumer with the opportunity, in a clear and conspicuous manner, to prohibit such disclosure. The video tape service provider may not disclose the title or description of any video tapes or other audio visual material. The subject matter of such materials may be disclosed only if the disclosure is for the exclusive use of marketing goods and services directly to the consumer, and if the consumer has been provided, in a clear and conspicuous manner, with the opportunity to prohibit such disclosure. Those who receive such a disclosure are themselves subject to the restrictions of the bill. *See* discussion of Section 2710(a)(4) above.

The committee intends that notice must be clear and conspicuous and must be given prior to disclosure being made. The phrase "clear and conspicuous manner" should be given its common sense meaning and may not be interpreted to allow "fine-print" notice on the reverse side of a business form, or other notice that a consumer is unlikely to see. Video tape service providers are encouraged to provide other kinds of notice that may help inform the consumer of his or her right to limit disclosure, such as a placard near a cash register for point-of-sale transactions or an additional notice for a direct mail solicitation.

This subsection carries forward the current market practice commonly known as a "negative option." It limits disclosure to the names and addresses of consumers to those circumstances in which consumers have been given the opportunity to prohibit any such disclosure. The video tape service provider, prior to disclosure and in a time frame that makes such notice meaningful, must provide an opportunity for the consumer to prohibit any such disclosure.

In addition, subsection (b)(2)(D)(ii) provides that for the exclusive use of marketing goods and services directly to the consumer, the video tape service provider may include in its disclosure of its customer lists the subject matter of the material bought or rented by those customers. Disclosure of subject matter may be made only in instances where communications are sent directly to the consumer. Some video tape service providers sell limited types of videos. For example, a golf shop may rent or sell golf videos, or a continuity club might rent or sell only Star Trek videos. The disclosure of the customer lists of those providers indirectly would disclose the subject matter of the video. Similarly, some video tape service providers market their video tapes in subject matter categories such as action, romance, science fiction and the like. These practices must be balanced against the consumer's right to privacy, and they con-

tinue to be limited by the consumer's prerogative to prohibit disclosure through the negative option procedures set forth above.

Under paragraph (2)(E), personally identifiable information may be disclosed if the disclosure is incident to the ordinary course of business of the video tape service provider. The circumstances that constitute the "ordinary course of business" are explicitly set out in subsection 2710(a)(2), and are limited to debt collection activities, order fulfillment, request processing, and the transfer of ownership.

The activities that constitute "ordinary course of business" are narrowly defined so as to avoid the possibility that a subsequent interpretation would undercut the purpose of this Act, as occurred with the phrase "routine use" in the 1974 Privacy Act.

This subsection takes into account that video tape service providers may use third parties in their business operations. For example, debt collection is often conducted by third parties, with disclosure of credit histories made to third party credit bureaus. Debt collection is subject to other Federal laws: disclosures for that purpose continue to be governed by those laws.

This subsection also allows disclsoure to permit video tape service providers to use mailing houses, warehouses, computer services, and similar companies for marketing to their customers. These practices are called "order fulfillment" and "request processing." In addition, when a business is sold, its customer list is often its most valuable asset. Any recipient of information under subsection (b)(2)(E) will be responsible under the statute for maintaining the confidentiality of the information as if he or she were the video tape service provider.

Under paragraph (2)(F), personally identifiable information may be disclosed pursuant to a court order in a civil proceeding, upon a showing of compelling need for the information that cannot be accommodated by any other means, and if (i) the consumer is given reasonable notice, by the person seeking the disclosure, of the court proceeding relevant to the issuance of the court order; and (ii) the consumer is afforded the opportunity to appear and contest the claim of the person seeking the disclosure.

This requirement for disclosure pursuant to court order in civil proceedings supersedes federal and state rules of discovery and would prevent disclosure pursuant to a court order in discovery proceedings unless that order complied with this subsection of the Act.

If personally identifiable information is disclosed, pursuant to paragraph (2)(F), the courts shall impose appropriate safeguards against unauthorized disclosure.

Section 2710(c) imposes liability where an individual, in violation of the Act, knowingly discloses personally identifiable information concerning any consumer. Under generally applicable principles of tort law, the action of an employee is generally imputed to the employer when the employee is found to have acted within the scope of his or her employment.

In making that determination, the court or jury, as the trier of fact, should consider all relevant facts, and the context in which they arise. For example, it may be relevant that the video tape

service provider has an explicit store policy that requires compliance with this Act.

To ensure compliance with the law, video tape service providers are urged to explain the federal law and the store's policy of compliance with it; warn their employees that disclosure of personal information by anyone not designated to do so on behalf of the business is grounds for dismissal; and post conspicuous notice of the law and store policy in plain view of all employees, such as at the customer counter and by the telephone.

This bill does not change current law regard to the liability of employees for acts committed within the scope of their employment.

Section 2710(d) is intended to apply to the situation when a private individual obtains personally identifiable information in violation of the Act. It is not intended to apply to any federal, state, or local governmental official. It states that such information shall not be received in evidence in any trial, hearing, arbitration, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a state, or a political subdivision of a state.

Section 2710(e) requires the destruction of personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information under subsections (b)(2) or (c)(2) or pursuant to a court order. The purpose of this provision is to reduce the chances that an individual's privacy will be invaded, by requiring the destruction of information in an expeditious fashion, appropriate to the circumstances and to the policies protected by this Act.

Under this subsection, the phrase the "purpose for which it was collected" must be narrowly construed. It may include only activities that are for the exclusive use of marketing goods and services to the consumer. It may not, however, include activities that violate the intent of the statute, which is to protect personally identifiable information from disclosure.

Section 2710(f) explicitly preserves the rights of consumers to seek redress under state laws that may provide a greater degree of protection than is afforded by the federal statute. The bill does not preempt state laws that provide greater privacy protection for video users.

VII. Cost Estimate

U.S. Congress,
Congressional Budget Office,
Washington, DC, October 14, 1988.

Hon. Joseph R. Biden, Jr.,
Chairman, Committee on the Judiciary,
U.S. Senate, Washington, DC.

Dear Mr. Chairman: The Congressional Budget Office has reviewed S. 2361, the Video Privacy Protection Act of 1988, as ordered reported by the Senate Committee on the Judiciary, October

5, 1988. Based on information from the Administrative Office of the U.S. Courts, we estimate that enactment of the bill would result in no significant cost to the federal government or to state or local governments.

S. 2361 would prohibit video tape service providers from disclosing personally identifiable information concerning consumers of such providers. This information could be disclosed only under special circumstances. The bill also would provide a civil remedy for aggrieved persons.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Mitchell Rosenfeld, who can be reached at 226-2860.

Sincerely,

JAMES L. BLUM,
Acting Director.

VIII. REGULATORY IMPACT STATEMENT

Pursuant to paragraph 11(b), rule XXVI of the Standing Rules of the Senate, the Committee, after due consideration, concludes that the bill will not have direct regulatory impact.

IX. CHANGES IN EXISTING LAW

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets; new matter is printed in italic; existing law in which no change is proposed is shown in roman):

UNITED STATES CODE

* * * * * * *

TITLE 18—CRIMES AND CRIMINAL PROCEDURE

* * * * * * *

CHAPTER 121—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

Sec.
2701. Unlawful access to stored communications.
2702. Disclosure of contents.
2703. Requirements for governmental access.
2704. Backup preservation.
2705. Delayed notice.
2706. Cost reimbursement.
2707. Civil action.
2708. Exclusivity of remedies.
2709. Counterintelligence access to telephone toll and transactional records.
2710. Wrongful disclosure of video tape rental or sale records.
[2710.] *2711* Definitions.

* * * * * * *

§ 2709. Counterintelligence access to telephone toll and transactional records

(a) DUTY TO PROVIDE.—A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

* * * * * * *

(e) REQUIREMENT THAT CERTAIN CONGRESSIONAL BODIES BE INFORMED.—On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests made under subsection (b) of this section.

§ 2710. Wrongful disclosure of video tape rental or sale records

(a) DEFINITIONS.—For purposes of this section—

(1) the term "consumer" means any renter, purchaser, or subscriber of goods or services from a video tape service provider;

(2) the term "ordinary course of business" means only debt collection activities, order fulfillment, request processing, and the transfer of ownership;

(3) the term "personally identifiable information" includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider or library; and

(4) the term "video tape service provider" means any person, engaged in the business of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials, or any person or other entity to whom a disclosure is made under paragraph (b)(2)(D), but only with respect to the information contained in the disclosure.

(b) VIDEO TAPE RENTAL AND SALE RECORDS.—(1) A video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for the relief provided in subsection (d).

(2) A video tape service provider may disclose personally identifiable information concerning any consumer—

(A) to the consumer;

(B) to any person with the informed, written consent of the consumer given at the time the disclosure is sought;

(C) to a law enforcement agency pursuant to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a grand jury subpoena, or a court order;

(D) to any person if the disclosure is solely of the names and addresses of consumers and if—

(i) the video tape service provider has provided the consumer with the opportunity, in a clear and conspicuous manner, to prohibit such disclosure; and

(ii) the disclosure does not identify the title, description, or subject matter of any video tapes or other audio visual

material; however, the subject matter of such materials may be disclosed if the disclosure is for the exclusive use of marketing goods and services directly to the consumer;

(E) to any person if the disclosure is incident to the ordinary course of business of the video tape service provider; or

(F) pursuant to a court order, in a civil proceeding upon a showing of compelling need for the information that cannot be accommodated by any other means, if—

(i) the consumer is given reasonable notice, by the person seeking the disclosure, or the court proceeding relevant to the issuance of the court order; and

(ii) the consumer is afforded the opportunity to appear and contest the claim of the person seeking the disclosure.

If an order is granted pursuant to subparagraph (C) or (F), the court shall impose appropriate safeguards against unauthorized disclosure.

(3) Court orders authorizing disclosure under subparagraph (C) shall issue only with prior notice to the consumer and only if the law enforcement agency shows that there is probable cause to believe that the records or other information sought are relevant to a legitimate law enforcement inquiry. In the case of a State government authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the video tape service provider, may quash or modify such order if the information or records requested are unreasonably voluminous in nature or if compliance with such order otherwise would cause an unreasonable burden on such provider.

(c) CIVIL ACTION.—(1) Any person aggrieved by any act of a person in violation of this section may bring a civil action in a United States district court.

(2) The court may award—

(A) actual damages but not less than liquidated damages in the amount of $2,500;

(B) punitive damages;

(C) reasonable attorneys' fees and other litigation costs reasonably incurred; and

(D) such other preliminary and equitable relief as the court determines to be appropriate.

(3) No action may be brought under this subsection unless such action is begun within 2 years from the date of the act complained of or the date of discovery.

(4) No liability shall result from lawful disclosure permitted by this section.

(d) PERSONALLY IDENTIFIABLE INFORMATION.—Personally identifiable information obtained in any manner other than as provided in this section shall not be received in evidence in any trial, hearing, arbitration, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision of a State.

(e) DESTRUCTION OF OLD RECORDS.—A person subject to this section shall destroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected

and there are no pending requests or orders for access to such information under subsections (b)(2) or (c)(2) or pursuant to a court order.

(f) SELECTION OF A FORUM.—Nothing in this section shall limit rights of consumers or patrons otherwise provided under State or local law. A federal court shall, in accordance with section 1738 of title 28, United States Code, give preclusive effect to the decision of any State or local court or agency in an action brought by a consumer or patron under a State or local law similar to this section. A decision of a Federal court under this section shall preclude any action under a State or local law similar to this section.

[§ 2710.] *§ 2711.* Definitions for chapter

As used in this chapter—

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and

(2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.

○